National Cybersecurity Strategy

Jose Rojas

School of Cybersecurity

CYSE 425W

Professor Duvall

November 5, 2023

National Cybersecurity Strategy

B.L.U.F

In the National Cybersecurity Strategy there are five pillars that are mentioned that will essentially help make the digital ecosystem we have created for ourselves using technology much safer, resilient, and aligned with our values. It talks about how digital technologies have increasingly touched the most sensitive aspects of our lives while providing convenience, it has also created new unforeseen risks.

National Cybersecurity Strategy

Cybersecurity is essential to the basic functioning of our economy. This includes our critical infrastructure, privacy of our data, and our national defense. The overall strategy approaches both the public sector and the private sector which is important because we would have to collaborate in order to protect cyberspace. Also the biggest information we could take from this is that the implementation plan calls for two fundamental shifts on how the United States allocates roles, responsibilities, and resources in cyberspace. These two are that they must ensure that the biggest and best positioned entities in the public and private sectors assume a greater share of the burden for mitigating cyber risk, and increasing incentives to favor long term investments into cybersecurity. Also it is important to mention the 5 pillars which are as follows: Pillar One | Defending Critical Infrastructure, Pillar Two | Disrupting and Dismantling Threat Actors, Pillar Three | Shaping Market Forces and Driving Security Resilience, Pillar Four | Investing in a Resilient Future, Pillar Five | Forging International Partnerships to Pursue Shared Goals. These are the pillars and we can talk a little about each one before choosing one to

directly talk more about, this would still be considered as a general overview. Each pillar has multiple steps to achieve its job but in this case for pillar one which is to defend the critical infrastructure this purpose of this pillar is to defend the systems and assets that help our national security, public safety and economic prosperity. The main goal of this pillar is to make the federal government's critical systems more defensible and resilient. They also want to build new and innovative capabilities that allow owners of critical infrastructure, federal agencies, and service providers to collaborate with each other so that they could have quicker response times. The second pillar is about disrupting and dismantling threat actors and this could be easily summarized by a statement used in the pdf. " The United States will use all instruments of national power to disrupt and dismantle threat actors
whose actions threaten our interests. These efforts may integrate diplomatic, information, military (both kinetic and cyber), financial, intelligence, and law enforcement capabilities." The third pillar talks about shaping market forces to drive security and resilience. The goal of this pillar is to make the digital economy promote practices that enhance the security and resilience of the digital ecosystem while preserving innovation and competition. The fourth pillar is to invest in a resilient future and this is the one we will dive deeper into because this one to me is interesting. The fifth pillar is to forge international partnerships to pursue shared goals, the goal of this would be to work with international countries to create a more reliable and secure internet.

The pillar I want to dive deeper into would be investing in a resilient future. This pillar has five objectives and these are to secure the foundation of the internet, reinvigorate federal research and development for cybersecurity, prepare for our post-quantum future, secure our clean energy future, support development of a digital identity ecosystem, and develop a national strategy to strengthen our cyber workforce. First I want to focus on strengthening the

cybersecurity workforce. The article states that the reality of this is that the United States will never have a sufficient cyber workforce within a huge investment in research related to automating many of the current human functions within cybersecurity. This goes to show the importance of cybersecurity and how jobs will continue to increase because the problem is just too big. What is really interesting to me is that the article also states that work is too tedious and the labor is too expensive and that the people who are extremely talented in cybersecurity should be focused on directing the automation that is performing the grunt work. This means that we are agreeing that artificial intelligence taking over even cybersecurity could be really dangerous, of course we already have tools that do our job for us that are also automated but that does not mean that humans should be filling jobs in cyber just for automation to come and do their job for them. Another important fact they talk about is that in this pillar the objective would also be to mitigate the border gateway protocol, unencrypted DNS requests, and slow the adoption of IPv6. The adoption of IPv6 is very interesting to me because this would be moving backwards instead of forward, IPv6 was made with security in mind so when configured and implemented correctly it can be more secure than IPv4. Personally I still do agree with mitigating the adoption of IPv6 but what's important is that IPv4 is running out of addresses so finding a way to mitigate that would be difficult unless we just switch completely to IPv6. I have worked in the tech field and during this time my coworkers would complain about IPv6 so from a technical point of view I can see why we do not want to make that switch yet even though it is the future and it would be considered moving forwards.

Conclusion

In conclusion this strategy has a great vision for the future of cyberspace. Not just across the United States but also at an international level. By collaborating with the public and private sectors this vision can be attainable, also realigning incentives to favor long term investments in the cybersecurity world. This will all help the internet as well as infrastructures to have a more secure cyberspace and can also create more jobs for the field. As everything is going digital in this generation we have to adapt and make sure that our digital ecosystem we have created is safe and reliable.

References

Allison, J. (2023, July 27). *National Cybersecurity Deep Dive: Invest in a resilient future and Forge International Partnerships* . Devo.com. https://www.devo.com/blog/national-cybersecurity-deep-dive-invest-in-a-resilient-future-and-forge-international-partnerships/

The United States Government. (2023, July 13). *Fact sheet: Biden-Harris Administration publishes the National Cybersecurity Strategy Implementation Plan*. The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/13/fact-sheet-biden-harrisadministration-publishes-thenational-cybersecurity-strategyimplementation-plan/

The White House. (n.d.). https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf?wpisrc=nl_cybersecurity202